MULTI-JURISDICTION PRIVACY STANDARDS

Data Protection Frameworks for Cross-Border Estates

November 2024

N. Rutland · F. Patterson

Engadin Institute
c/o 1209 Orange Street
Wilmington, DE 19801
United States

We protect objects from weather and noise. Not from society.

ABSTRACT

Cross-border wealth management operations face systematic compliance challenges from conflicting data protection regimes. This paper analyzes privacy law requirements across major wealth jurisdictions and proposes harmonized compliance protocols. Problem Statement: UHNW families and advisors operating across multiple jurisdictions must comply with:

- EU GDPR (extraterritorial application)
- UK GDPR (post-Brexit divergence)
- US state privacy laws (California CCPA, Virginia VCDPA, 14+ others)
- Swiss Federal Data Protection Act (FADP)
- Singapore Personal Data Protection Act (PDPA)

These regimes conflict on:

- Lawful basis for processing (consent vs legitimate interest)
- Cross-border transfer mechanisms
- Data subject rights (access, deletion, portability)
- Controller vs processor obligations
- Breach notification requirements
- Penalties (GDPR: 4% global revenue; US: $7,500 per violation)

Result: Compliance paralysis or systematic violation risk. **Proposed Framework:** The Multi-Jurisdiction Privacy Standard (MJPS) establishes:

1. **Highest common standard** approach (comply with strictest regime)
2. **Data minimization protocols** (collect less = less compliance burden)
3. **Jurisdiction mapping** (which law applies to which data)
4. **Cross-border transfer safe harbors** (SCCs, BCRs, adequacy decisions)
5. **Breach response protocols** (72-hour notification, multi-jurisdiction)

Scope: Analysis covers wealth management operations including:

- Client relationship management (CRM systems)
- Estate documentation (wills, trusts, financial records)
- Advisor communications (email, document sharing)
- Cross-border service delivery (multi-jurisdiction families)

THE MULTI-JURISDICTION COMPLIANCE PROBLEM

I. CONFLICTING PRIVACY REGIMES

Case Study UK Family, Swiss Advisor, US Assets

Facts:

- Family: UK resident, British citizens
- Advisor: Wealth management firm, Switzerland
- Assets: 40% US (real estate, investments), 30% UK, 30% Switzerland
- Estate planning: Cross-border trust structure

Data flows:

- UK family -> Swiss advisor (client data transfer)
- Swiss advisor -> US legal counsel (estate planning)
- Swiss advisor -> UK solicitor (probate planning)
- US investment platform -> Swiss advisor (account statements)

Applicable privacy laws:

- **UK GDPR:** Applies to UK family's personal data
- **Swiss FADP:** Applies to Swiss advisor (data controller)
- **US state laws:** California CCPA applies if family has California assets
- **EU GDPR:** May apply via extraterritorial effect

Compliance questions: 1. Lawful basis for processing:

- **UK GDPR:** Legitimate interest? Contract? Consent?
- **Swiss FADP:** Legitimate purpose required
- **California CCPA:** Opt-out right (different from GDPR consent)

2. Cross-border transfer:

- UK -> Switzerland: Adequacy decision exists (Switzerland "adequate")
- Switzerland -> US: Standard Contractual Clauses required
- US -> UK: UK GDPR restrictions on transfers to "third countries"

3. Data subject rights:

- **UK GDPR:** Right to erasure ("right to be forgotten")
- **Swiss FADP:** Right to correction, no explicit erasure right
- **California CCPA:** Right to deletion (with business exceptions)

4. Retention:

- **UK:** Tax records 6 years (HMRC)

- **Switzerland:** Business records 10 years (commercial law)
- **US:** IRS records 3-7 years (varies by document type)

Result: Advisor must comply with longest retention (10 years) while honoring deletion requests (conflict).

Failure Scenario

What happened:

- Swiss advisor failed to implement proper cross-border transfer mechanisms
- UK regulator (ICO) investigation: £50,000 fine
- Swiss regulator (FDPIC): Warning + audit requirement
- California: No enforcement (yet) but exposure remains

Cost:

- Direct fines: £50k
- Legal fees: £120k (multi-jurisdiction compliance audit)
- Remediation: £80k (new systems, SCCs, policies)
- Reputational damage: 3 client losses (£2M AUM)

Total: £250k+ cost for non-compliance **Prevention cost:** £15k-£30k (proper compliance framework) **Lesson:** Multi-jurisdiction compliance is not optional.

GDPR FRAMEWORK EUUK

II. GDPR: THE DOMINANT PRIVACY REGIME

Key Principles Article 5 GDPR

1. Lawfulness, fairness, transparency

- Must have lawful basis (consent, contract, legitimate interest, etc.)
- Processing must be fair to data subject
- Transparent privacy notices required

2. Purpose limitation

- Data collected for specified purposes only
- Cannot repurpose without new lawful basis

3. Data minimization

- Collect only data necessary for purpose
- "Nice to have" ≠ lawful collection

4. Accuracy

- Data must be accurate and kept up to date
- Duty to correct inaccurate data

5. Storage limitation

- Retain only as long as necessary
- Must have retention schedule and deletion protocols

6. Integrity and confidentiality

- Appropriate security measures
- Protect against unauthorized access, loss

7. Accountability

- Must demonstrate compliance
- Document decisions, policies, procedures

Lawful Basis for Wealth Management

Option 1: Consent (Article 6(1)(a))

- **Pros:** Clear, explicit client agreement
- **Cons:** Client can withdraw anytime (disrupts service)
- **Use case:** Marketing, non-essential processing

Option 2: Contract (Article 6(1)(b))

- **Pros:** Processing necessary for service delivery
- **Cons:** Limited to contract performance only
- **Use case:** Client onboarding, account management

Option 3: Legitimate Interest (Article 6(1)(f))

- **Pros:** Flexible, balances advisor needs with client rights
- **Cons:** Requires Legitimate Interest Assessment (LIA)
- **Use case:** Fraud prevention, internal recordkeeping

Wealth management firms typically rely on:

- **Contract** (primary): Account management, advice delivery
- **Legitimate interest** (secondary): Risk management, compliance
- **Legal obligation** (6(1)(c)): AML/KYC, tax reporting

Data Subject Rights Articles 15-22

Right of access (Article 15):

- Client can request copy of all their data
- Must respond within 1 month
- Must be free (unless excessive/unfounded)

Right to rectification (Article 16):

- Client can correct inaccurate data
- Advisor must update within reasonable time

Right to erasure (Article 17) - "Right to be Forgotten":

- Client can request deletion
- **Exceptions:** Legal obligation (e.g., AML records), establishment of legal claims
- **Wealth management challenge:** Retention requirements vs erasure requests

Right to restriction (Article 18):

- Client can limit processing (e.g., during accuracy dispute)
- Data stored but not actively processed

Right to data portability (Article 20):

- Client can receive data in machine-readable format
- Transfer to another advisor (switching facilitation)

Right to object (Article 21):

- Client can object to processing based on legitimate interest
- Advisor must stop unless compelling grounds override

Cross-Border Transfers Chapter V GDPR

Problem:

- GDPR restricts transfers to "third countries" (non-EU/EEA)
- UK is now "third country" post-Brexit (though adequacy decision exists)
- US is "third country" (no adequacy, except Data Privacy Framework for some companies)

Transfer mechanisms: 1. Adequacy decision (Article 45):

- EU Commission deems country has adequate protection
- Transfers allowed as if within EU
- **Countries:** Switzerland, UK, Japan, Canada (commercial), Argentina, Israel
- **US:** DPF (Data Privacy Framework) for certified companies only

2. Standard Contractual Clauses (Article 46(2)(c)):

- EU Commission-approved contract templates
- Importer commits to GDPR-equivalent protections
- **Use case:** Transfers to US (non-DPF), Asia, most countries

3. Binding Corporate Rules (Article 47):

- Internal group transfer mechanism
- Requires regulatory approval
- **Use case:** Large multinational wealth managers

4. Derogations (Article 49):

- Explicit consent (for specific transfer)
- Necessary for contract performance
- **Limited use** (strict interpretation)

US PRIVACY LAW LANDSCAPE

III. US STATE PRIVACY LAWS

The Fragmented US Regime

No federal comprehensive privacy law (as of 2024) State laws (16+ enacted):

- California: CCPA (2020), CPRA (2023)
- Virginia: VCDPA (2023)
- Colorado: CPA (2023)
- Connecticut: CTDPA (2023)
- Utah: UCPA (2023)
- + 11 more states (2024)

Each law differs on:

- Scope (who's covered)
- Consumer rights
- Opt-in vs opt-out
- Penalties
- Private right of action

California CCPACPRA Strictest, Most Relevant

Scope:

- Applies to businesses that:
- Annual gross revenue >$25M, OR
- Buy/sell personal info of 100k+ consumers, OR
- Derive 50%+ revenue from selling personal info

Wealth managers:

- Likely covered if serve California clients
- Even if not California-based (extraterritorial)

Consumer rights: Right to know (§1798.100):

- What personal info collected
- Sources, purposes, categories of third parties shared with

Right to delete (§1798.105):

- Request deletion of personal info
- **Exceptions:** Legal obligations, fraud prevention, security

Right to opt-out of sale (§1798.120):

- "Sale" broadly defined (includes sharing for value)
- Must have "Do Not Sell My Personal Information" link

Right to correction (CPRA addition):

- Correct inaccurate personal info

Right to limit use of sensitive personal info (CPRA):

- "Sensitive" = financial info, precise geolocation, health data
- Wealth management data likely "sensitive"

Obligations: Privacy notice:

- Must disclose categories of info collected
- Purposes, third-party sharing
- Consumer rights

Opt-out mechanisms:

- "Do Not Sell" link on website
- Must honor requests within 15 days

Authorized agent:

- Must accept requests via authorized representative

Non-discrimination:

- Cannot deny service for exercising rights
- Can offer financial incentive for NOT exercising rights (if disclosed)

Penalties:

- **Civil:** $2,500 per violation (unintentional), $7,500 (intentional)
- **Private right of action:** Data breach only ($100-$750 per consumer)

Enforcement:

- California Attorney General (primary)
- California Privacy Protection Agency (CPPA - created by CPRA)

CCPA vs GDPR Comparison

Aspect	GDPR	CCPA
Lawful basis	Required (6 bases)	Not required
Consent	Opt-in (affirmative)	Opt-out (sale of data)
Deletion	Right to erasure	Right to delete

Portability	Right to data portability	Right to know (less portable)
Scope	Personal data	Personal information (broader)
Penalties	4% global revenue	$2,500-$7,500 per violation
Regulator	National DPAs	Attorney General + CPPA

SWISS DATA PROTECTION

IV. SWISS FADP (Federal Act on Data Protection)

Revised FADP Effective September 2023

Key changes:

- Aligns closer to GDPR (but not identical)
- Expanded data subject rights
- Mandatory data breach notification
- Higher penalties (CHF 250,000)

FADP Principles

Lawfulness and good faith (Article 6):

- Processing must be lawful
- Must not be misleading or unconscionable

Proportionality (Article 6):

- Data collected must be proportionate to purpose
- Similar to GDPR data minimization

Purpose limitation (Article 6):

- Process only for purposes disclosed at collection
- Cannot repurpose without consent

Accuracy (Article 6):

- Data must be accurate
- Duty to correct errors

Retention (Article 6):

- Retain only as long as necessary
- Must have deletion/archiving protocols

Data Subject Rights

Right of access (Article 25):

- Can request confirmation of processing
- Can request copy of data

Right to correction (Article 32):

- Can request correction of inaccurate data

Right to object (Article 30):

- Can object to processing (limited grounds)

No explicit right to erasure:

- Unlike GDPR, FADP has no "right to be forgotten"
- But proportionality + retention limits may require deletion

---

Cross-Border Transfers

Countries with adequate protection (Article 16):

- EU/EEA (via adequacy decision)
- UK (post-Brexit adequacy maintained)
- Other countries: Case-by-case (no published adequacy list)

Transfer mechanisms (Article 16):

- Standard Contractual Clauses (similar to GDPR SCCs)
- Binding Corporate Rules
- Explicit consent

US transfers:

- No adequacy decision
- Require SCCs or other safeguards

Wealth Management Implications

Swiss banks/advisors:

- Often serve cross-border clients (EU, UK, US)
- Must comply with FADP + client jurisdiction law
- GDPR extraterritorial application (if serving EU clients)

Key compliance requirements:

- Privacy notice (must inform about cross-border transfers)
- Cross-border transfer mechanisms (SCCs for US, adequacy for EU/UK)
- Data subject rights (access, correction)
- Breach notification (within 72 hours - new requirement)

HARMONIZED COMPLIANCE FRAMEWORK

V. MULTI-JURISDICTION PRIVACY STANDARD (MJPS)

Principle 1 Highest Common Standard

Approach: Identify strictest requirement across all applicable jurisdictions and comply with that standard globally. **Example: Deletion requests:**

- GDPR: Right to erasure (with exceptions)
- CCPA: Right to delete (with exceptions)
- Swiss FADP: No explicit right, but proportionality may require

MJPS standard: Honor deletion requests unless:

- Legal retention requirement (tax, AML)
- Necessary for legal claims defense
- Necessary for contract performance

Implement globally (not jurisdiction-specific). **Advantage:**

- Simplifies operations (one policy, not 5+)
- Reduces error risk (staff don't choose "which law applies")
- Future-proofs (new strict law? Already compliant)

Disadvantage:

- May exceed legal minimum (compliance cost)
- But cost < risk of multi-jurisdiction violation

Principle 2 Data Minimization

Strategy: Collect less data = less compliance burden. Wealth management often over-collects:

- Full financial statements (when summary sufficient)
- Entire family tree (when immediate beneficiaries only relevant)
- Historical documents (when current status only needed)

MJPS approach: Before collecting any data, ask:

1. Is this necessary for service delivery? (GDPR Article 5(1)(c))
2. Is there less intrusive alternative?
3. How long will we need this?

Example: Traditional: Collect full bank statements (50 pages/month × 12 = 600 pages/year) **Minimized:** Collect summary statement (account name, balance, owner) = 1 page **Result:**

- 99% less data stored

- 99% less risk (breach, deletion request, retention)
- Same service quality

Principle 3 Jurisdiction Mapping

Problem: Multi-jurisdiction families -> which law applies to which data? **Solution: Create data jurisdiction map:**

Data Type	Subject	Storage Location	Applicable Law
Client profile	UK citizen	Switzerland	UK GDPR, Swiss FADP
US property docs	UK citizen	Switzerland	UK GDPR, Swiss FADP, California CCPA
Swiss account statements	UK citizen	Switzerland	UK GDPR, Swiss FADP
Advisor notes	UK citizen	Switzerland	Swiss FADP, UK GDPR

Then:

- Identify strictest law per data type
- Implement controls for that standard
- Document decision (accountability)

Principle 4 Purpose-Specific Processing

GDPR Article 5(1)(b): Purpose limitation Avoid:

- Vague purpose ("business operations")
- Open-ended retention ("until client leaves")

Do:

- Specific purpose ("estate planning advice")
- Defined retention ("10 years post-relationship, then deletion unless legal hold")

MJPS template:

```
DATA PROCESSING RECORD
Data Category: [e.g., Financial account statements]
Purpose: [e.g., Tax planning advice]
Lawful Basis: [e.g., Contract - necessary for advice delivery]
Retention: [e.g., 10 years post-relationship (Swiss commercial law)]
Access: [e.g., Advisor, compliance officer only]
Cross-Border: [e.g., May transfer to UK solicitor via SCCs]
Deletion: [e.g., Automatic after retention period unless legal hold]
```

Repeat for each data category. Advantage:

- Defensible processing (can demonstrate compliance)
- Limits scope creep (staff can't repurpose data)

- Facilitates deletion (know when to purge)

CROSS-BORDER TRANSFER PROTOCOLS

VI. SAFE CROSS-BORDER DATA FLOWS

Standard Contractual Clauses SCCs Implementation

When required:

- Transfer from EU/UK to non-adequate country (e.g., US, Singapore, most of world)
- Swiss FADP also requires SCCs for non-adequate countries

How to implement: Step 1: Identify transfers

- List all cross-border data flows
- Determine if adequacy decision covers (EU -> Switzerland: yes; EU -> US: no)

Step 2: Select SCC module

- Module 1: Controller to controller
- Module 2: Controller to processor
- Module 3: Processor to processor
- Module 4: Processor to controller

Wealth management typical: Module 1 (advisor to advisor) or Module 2 (advisor to service provider) **Step 3: Execute SCCs**

- Both parties sign
- Incorporate into service agreement or standalone
- File in compliance records

Step 4: Transfer Impact Assessment (TIA)

- **Required post-Schrems II:** Assess if destination country law undermines SCC protections
- **US transfers:** Evaluate FISA 702, EO 12333 risks
- Document assessment

Step 5: Supplementary measures (if needed)

- Encryption in transit and at rest
- Pseudonymization
- Technical measures to prevent government access

Data Privacy Framework DPF Alternative US Only

For US companies:

- Can self-certify to EU-US Data Privacy Framework
- Replaces invalidated Privacy Shield

- EU Commission adequacy decision (July 2023)

If US service provider DPF-certified:

- No SCCs required for EU -> US transfer
- Simpler compliance (just verify certification)

Verification:

- Check DPF list: https://www.dataprivacyframework.gov/list
- Confirm company + services covered

Limitations:

- Only covers US companies (not other countries)
- Swiss-US DPF separate (check Swiss DPF list)
- Subject to legal challenges (Schrems III pending?)

UK-Specific International Data Transfer Agreement IDTA

UK alternative to EU SCCs:

- UK International Data Transfer Agreement (IDTA)
- OR use EU SCCs with UK Addendum

Which to use:

- IDTA: Simpler for UK-only transfers
- EU SCCs + UK Addendum: If also transferring from EU

Wealth managers serving UK + EU clients:

- Recommended: EU SCCs + UK Addendum (covers both)

BREACH NOTIFICATION PROTOCOLS

VII. MULTI-JURISDICTION BREACH RESPONSE

Notification Timelines

Jurisdiction	Regulator Notification	Individual Notification
EU GDPR	72 hours (Article 33)	Without undue delay (Article 34)
UK GDPR	72 hours	Without undue delay
Swiss FADP	ASAP (Article 24)	If high risk
California CCPA	Not specified	Without unreasonable delay
Other US states	Varies (24-90 days)	Varies

Strictest standard: 72 hours (GDPR) MJPS approach: Notify all applicable regulators within 72 hours.

Breach Response Protocol

Hour 0-2: Containment

- [ ] Identify breach scope (what data, how many subjects)
- [ ] Contain breach (stop unauthorized access)
- [ ] Preserve evidence (logs, forensics)

Hour 2-24: Assessment

- [ ] Determine applicable jurisdictions (where are data subjects?)
- [ ] Assess breach severity (high risk to data subjects?)
- [ ] Determine if notification required (or exception applies)
- [ ] Draft notification text

Hour 24-72: Notification

- [ ] Notify all applicable regulators (GDPR, UK, Swiss, US states)
- [ ] Use regulator-specific forms/portals where required
- [ ] Document notification (keep proof of submission)

Hour 72+: Individual Notification

- [ ] If high risk: Notify affected individuals
- [ ] Provide mitigation steps (password reset, credit monitoring)
- [ ] Ongoing communication as investigation progresses

Multi-Jurisdiction Notification Template

To Regulators:

```
PERSONAL DATA BREACH NOTIFICATION
1. DATA CONTROLLER:
2. DATA PROTECTION OFFICER (if applicable):
3. BREACH DETAILS:
Date/time discovered: [timestamp]
Nature of breach: [unauthorized access / loss / disclosure]
Categories of data: [financial info, identification, etc.]
Approximate number affected: [number]
4. LIKELY CONSEQUENCES:
5. MEASURES TAKEN:
6. INDIVIDUAL NOTIFICATION:
7. CROSS-BORDER ELEMENT:
This breach affects data subjects in: [list jurisdictions]
Notifications submitted to: [list regulators]
```

Submit to:

- ICO (UK): Via ICO portal
- EU DPAs: Via national DPA (CNIL for France, etc.)
- FDPIC (Switzerland): Via email/portal
- US state AGs: Per state-specific procedures

PRACTICAL COMPLIANCE TOOLKIT

VIII. IMPLEMENTATION GUIDANCE

Privacy Notice Template Multi-Jurisdiction

Required disclosures: 1. Data Controller Identity

```
[Company Name] is the data controller for your personal information.
Registered office: [Address]
Contact: [Email, phone]
Data Protection Officer: [Name, email] (if required)
```

2. Data Collected

```
We collect:
- Identification data (name, DOB, passport)
- Financial data (account details, holdings, income)
- Contact data (address, email, phone)
- Professional data (occupation, source of wealth)
```

3. Purposes and Lawful Basis

```
We process your data for:
- Wealth management services (Lawful basis: Contract)
- Regulatory compliance (Lawful basis: Legal obligation)
- Fraud prevention (Lawful basis: Legitimate interest)
```

4. Recipients

```
We may share your data with:
- Professional advisors (solicitors, accountants)
- Regulators (FCA, tax authorities)
- Service providers (technology, custody)
Cross-border transfers: We transfer data to [list countries].
Safeguards: Standard Contractual Clauses / Adequacy decision.
```

5. Retention

```
We retain your data for:
- Relationship period + 10 years (regulatory requirement)
- Tax records: 6 years (UK), 10 years (Switzerland)
After retention period: Data securely deleted unless legal hold.
```

6. Your Rights

```
You have the right to:
- Access your data (Article 15 GDPR)
- Correct inaccurate data (Article 16 GDPR)
- Request deletion (Article 17 GDPR - exceptions apply)
- Restrict processing (Article 18 GDPR)
- Data portability (Article 20 GDPR)
- Object to processing (Article 21 GDPR)
- Withdraw consent (if processing based on consent)
California residents: Right to opt-out of sale (we do not sell data).
To exercise rights: [Email, address, online form]
```

7. Complaints

```
You may lodge a complaint with:
- UK: Information Commissioner's Office (ICO)
```

```
- EU: Your national data protection authority
- Switzerland: Federal Data Protection Commissioner (FDPIC)
- US: State Attorney General (California, etc.)
```

Data Subject Rights Request Protocol

Request received:

- [ ] Verify identity (passport copy, account verification)
- [ ] Determine which right exercised (access, deletion, etc.)
- [ ] Identify applicable jurisdiction (GDPR, CCPA, etc.)
- [ ] Set deadline (1 month GDPR, 45 days CCPA)

Access request:

- [ ] Compile all data (systems, backups, emails)
- [ ] Redact third-party data (if present)
- [ ] Provide in accessible format (PDF, spreadsheet)
- [ ] Deliver within deadline

Deletion request:

- [ ] Verify no legal retention requirement
- [ ] Delete from production systems
- [ ] Delete from backups (or flag for deletion on backup rotation)
- [ ] Confirm deletion to data subject

Objection/restriction:

- [ ] Assess grounds (GDPR: compelling legitimate grounds to continue?)
- [ ] If no grounds: Stop processing
- [ ] If grounds exist: Explain to data subject

ADVISOR COMPLIANCE CHECKLIST

IX. WEALTH ADVISOR COMPLIANCE PROGRAM

Annual Compliance Tasks

Q1 (January-March):

- [ ] Review privacy notice (update if law changes)
- [ ] Audit data inventory (what data held, where)
- [ ] Review cross-border transfers (SCCs current? TIA up to date?)
- [ ] Staff privacy training (GDPR refresher)

Q2 (April-June):

- [ ] Test data subject rights procedures (mock access request)
- [ ] Review retention schedule (delete data per schedule)
- [ ] Vendor audit (do processors comply with DPA?)
- [ ] Update Records of Processing Activities (ROPA)

Q3 (July-September):

- [ ] Security assessment (penetration test, vulnerability scan)
- [ ] Breach response drill (test notification procedures)
- [ ] Review consent records (if using consent as lawful basis)
- [ ] Update Data Protection Impact Assessments (if needed)

Q4 (October-December):

- [ ] Year-end data purge (delete data beyond retention)
- [ ] Compliance report to board/management
- [ ] Budget for next year privacy program
- [ ] Monitor regulatory developments (new laws, guidance)

Technology Requirements

Minimum:

- Encrypted storage (at rest)
- Encrypted transmission (TLS 1.2+)
- Access controls (role-based, MFA)
- Audit logging (who accessed what, when)
- Backup encryption

Recommended:

- Data loss prevention (DLP)

- Pseudonymization (where feasible)
- Privacy-preserving analytics (aggregate, not individual)
- Automated retention/deletion

Gold standard:

- End-to-end encryption (zero-knowledge)
- Homomorphic encryption (process encrypted data)
- Differential privacy (statistical privacy guarantees)
- Privacy-by-design architecture

LIMITATIONS DISCLAIMERS

X. LIMITATIONS This document: Provides legal analysis, not legal advice:

- Privacy law is complex and jurisdiction-specific
- Professional legal counsel should be engaged for specific situations
- Does not create attorney-client relationship

Reflects law as of November 2024:

- Privacy law evolves rapidly (new state laws, EU guidance, court decisions)
- GDPR interpretation still developing (cases ongoing)
- US comprehensive federal privacy law possible (would change landscape)

Focuses on major jurisdictions:

- Analysis covers EU, UK, US, Switzerland primarily
- Other jurisdictions (Asia-Pacific, Latin America, Africa) have privacy laws not covered here
- Multi-national operations may require additional analysis

Does not address all scenarios:

- Specific industry requirements (e.g., financial services additional rules)
- Criminal investigations (law enforcement data access)
- National security (government surveillance)
- Sector-specific laws (HIPAA for health, FERPA for education)

Professional consultation recommended for: Complex cross-border operations:

- Offices in 3+ countries
- Clients in 5+ jurisdictions
- High-volume cross-border transfers

High-risk processing:

- Large-scale processing (10,000+ data subjects)
- Sensitive data (health, biometric, political views)
- Automated decision-making (profiling, algorithms)

Regulatory inquiries:

- Data protection authority investigations
- Breach notification requirements
- Cross-border transfer assessments

Privacy program design:

- Binding Corporate Rules (BCRs)

- Data Protection Impact Assessments (DPIAs)
- Privacy-by-design architecture

CONCLUSION

Multi-jurisdiction privacy compliance is not optional for cross-border wealth management. The compliance burden is real:

- EU GDPR: 4% global revenue penalties
- US state laws: $2,500-$7,500 per violation
- Switzerland: CHF 250,000 penalties
- Reputational damage: Client loss, regulatory scrutiny

Traditional approach (ignore or minimally comply) = systematic violation risk.

The Multi-Jurisdiction Privacy Standard (MJPS) provides framework: 1. Highest common standard

- Comply with strictest regime globally
- Simplifies operations, reduces error risk

2. Data minimization

- Collect less = less risk
- Challenge every data collection ("do we really need this?")

3. Jurisdiction mapping

- Know which law applies to which data
- Document decisions (accountability)

4. Cross-border safeguards

- SCCs for non-adequate countries
- Transfer Impact Assessments
- DPF certification where available

5. Breach readiness

- 72-hour notification capability
- Multi-jurisdiction templates
- Regular drills

Implementation cost: DIY (small firm):

- Privacy notice drafting: £500-£1,500
- SCCs implementation: £1,000-£3,000
- Staff training: £500-£1,000/year
- **Total: £2,000-£5,500 initial + £500-£1,000 annual**

Professional (mid-size firm):

- Privacy counsel retainer: £10k-£30k/year
- Technology (DLP, encryption): £5k-£20k
- Staff (privacy officer): £40k-£80k/year
- **Total: £55k-£130k annual**

Cost of non-compliance:

- GDPR fine: Up to 4% global revenue (£200k-£5M+ for wealth manager)
- US state fines: $2,500 × violations (can be £100k+ for systemic issues)
- Legal defense: £50k-£200k
- Client loss: Incalculable

ROI: 10-100× (compliance cost vs violation risk)

The privacy compliance gap is closing globally. Firms that act now:

- Avoid regulatory enforcement (first-mover compliance advantage)
- Build client trust (privacy = differentiator)
- Future-proof operations (new laws? Already compliant)

Firms that wait:

- Face enforcement risk (regulators active, penalties increasing)
- Lose clients (privacy-conscious UHNW increasingly demanding)
- Scramble to comply (expensive retrofit vs designed-in compliance)

The choice is clear.

REFERENCES:

[1] EU GDPR (Regulation 2016/679)
[2] UK GDPR (Data Protection Act 2018, as amended)
[3] Swiss Federal Data Protection Act (FADP, revised 2023)
[4] California Consumer Privacy Act (CCPA, 2020) and California Privacy Rights Act (CPRA, 2023)
[5] European Data Protection Board (EDPB) Guidelines 2/2018 on derogations (transfers)
[6] EDPB Recommendations 01/2020 on Transfer Impact Assessments (Schrems II)

FOOTER:

LP-02: Multi-Jurisdiction Privacy Standards | Page X of 16 | Engadin Institute | Legal Paper

---

Published by Standard Index Group Ltd · standardindex.group